Y2K Best Practices/Lessons Learned

Awareness

Awareness and education is the foundation of the BOP efforts to address the Y2K problem. Awareness and education activities have focused on the provision of information of the potential consequences of Y2K to equipment and systems operations, and dispelling any notions that Y2K is only a computer programming issue.

The general consensus during the development of these efforts was that there existed a basic understanding of certain kinds of disruptions Y2K could bring, that is the inability of software to process dates after December 31, 1999 could lead to software failures. However, there was more uncertainty that an understanding existed that Y2K potentially posed much more than a computer programming problem. Specifically, much of the original Y2K media focus appeared to be concerning the failure of computer programs, not failure of embedded systems. Efforts were made to eliminate this misconception by communications to staff of explicit examples of embedded systems that were subject to be affected by Y2K.

Efforts were also made to share a number of Y2K resources with staff. Material prepared by the Department of Justice and the General Services Administration (GSA) was disseminated as part of the communication efforts. Additionally, the BOP Web page was modified to provide links to Internet sites providing Y2K information.

Executive Management/Cross Agency Buy-in to the Issues

Executive management of efforts in the area of Y2K have been in the form of a structure involving staff from all disciplines within the BOP. The Assistant Director, Administration Division was named to be the BOP’s Senior Management Official for Y2K. The Senior Management Official chairs a work group consisting of two Y2K program managers, one with the responsibility for Information Transfer (IT) systems, the other with responsibility for non-IT systems. The remaining members of the work group represent each of the eight divisions within the Central Office of the BOP. All of the professional disciplines found in each BOP institution are represented by one of these Central Office Divisions.

Specific Y2K tasks are delegated to work group members, with each member given the latitude to assess the best way to accomplish the task within the disciplines covered by their division. This approach has allowed use of existing frameworks for the flow of information in the Y2K effort in lieu of developing a new structure solely for Y2K program management. This enables work group members to concentrate on the dissemination and gathering of necessary information with a minimum amount of time spent on the mechanics of the communications.

Work group members often rely upon specialists within their division, regional office staff, and institution staff. This approach has had several benefits. The first benefit is the ability for staff who would most likely be affected by any disruptions due to Y2K to be involved in the BOP’s efforts to minimize the likelihood of such occurrences. The second benefit is that this approach has allowed greater awareness of Y2K implications by involving more staff in these efforts.

Inventories

One of the largest tasks confronted by the BOP was the compilation of an accurate inventory of embedded systems. The goal was the creation of a database containing specific information on embedded systems subject to problems arising from Y2K.

The Y2K Senior Management Official prepared a memorandum for all Assistant Directors for each Central Office Division, all Regional Directors, and all institution Chief Executive Officers. This correspondence provided an overview of the type of systems potentially affected by Y2K, and help to dispel any misconceptions that Y2K only involved computer programming applications. Format for the information sought to develop the inventory was prescribed, but the manner used for collection was left to the discretion of the particular entity, allowing for the use of existing organizational structures, where appropriate.

Specific information for each system potentially affected by Y2K included:

- Equipment
- Manufacturer
- Model Number
- Serial Number
- Software Version/Controller Version (if applicable)
- Department Responsible for Equipment
- Y2K Compliance Status (if known)

This information was used to formulate a database containing this information. This database was used to identify potential gaps in information, and these gaps were filled with requests sent to specific sites for specific information. The database also allowed for sorting of information based on the department identified as being responsible for the equipment, and the delegation of any follow-up activities to the appropriate Division Representative on the Y2K work group. These efforts have also allowed for the creation of a central database providing an inventory of equipment and systems that can potentially be used for purposes beyond Y2K.

The updating of the inventory has been an on-going process, and will continue until all equipment and systems are identified as Y2K compliant, upgraded, or replaced.

Remediation/Replacement

The compilation of the database cataloging the inventory of equipment and systems potentially affected by Y2K has allowed for the identification of what measures, if any, need to be taken to assure Y2K compliance. Essentially, these actions take the form of replacement, upgrade, or relocation to an application where Y2K compliance is not an issue.

The key task in the process of selecting the appropriate action is the determination of whether the equipment or system is mission critical. A non-Y2K compliant mission critical system may still operate with only certain features affected. It must be ascertained if the loss of these features hinders the performance of a mission critical task. This finding serves as the basis for the determination of which of the three options for handling Y2K non-compliance are viable.

Replacement is the most costly option to rectify non-Y2K compliant systems. This option is mandated when Y2K non-compliance disrupts operation of a system that is mission critical where upgrading the system is either not an option or not cost-effective. Replacement may be necessitated where upgrades are not available, for instance, where the manufacturer does not provide an upgrade. Similarly, replacement may be mandated over an upgrade where, due to other considerations such as age of the existing system, it is more beneficial to invest in new equipment in lieu of addressing the Y2K compliance issue in a system that is borderline obsolete for other reasons. Additionally, some systems may already have been scheduled for replacement without regard to Y2K compliance.

Upgrade of a system to bring it into Y2K compliance is an option in many instances. An example would be a system that, except for Y2K non-compliance, is still capable of performing its function. This option is not only dependent upon the continued value of the system, but also upon the availability of an upgrade and the cost of the upgrade compared to replacement.

Relocation, in a sense, is replacement with the system relocated in lieu of being disposed. An example of where this would be a viable option would be the circumstance where the system's non-Y2K compliance does not affect certain functions, and these non-affected functions are comprehensive enough to allow continued use of the system in another application. Specifically, if there are two similar systems, one Y2K compliant and the other Y2K non-compliant, and the Y2K non-compliance of the second system only affects the accuracy of a date supplied on a report, and if the date is only needed for the function being performed by the Y2K compliant system, the systems could be interchanged.

Care must be taken in the determination of which option to pursue. Considerations beyond Y2K may assist in the selection of the appropriate option.

Testing

Testing has taken two forms in the BOP. These forms may be categorized as informal and formal.

Informal testing is exemplified by staff simply testing to see if systems will accept dates after December 31, 1999, and remain operable. This testing can be done by line staff. Only limited guidance is needed to instruct staff on how to carry out these types of tests. Equipment subject to this type of testing would typically be smaller, non-integrated systems where acceptable results would be apparent.

Formal testing is more applicable to larger systems, and those integrated where the Y2K non-compliance may not be immediately apparent. An example would be building systems with integrated controls. Here, the danger would be that acceptance of a date after December 31, 1999 may appear to not alter system performance, but due to the integration of several systems, could cause an operational disruption. The BOP has retained professional services to perform limited formal testing of select large and integrated systems.

Experience with Vendors

One of the first tasks undertaken following the original compilation of the inventory was contacting vendors to ascertain their products' Y2K compliance status. The level of response has been as varied as the systems under investigation. This problem has been compounded by some manufacturers ceasing to do business, and by mergers and take-overs. However, the approach of sending correspondence to manufacturers and telephone contacts has provided the bulk of confirmation regarding Y2K concerns, Y2K compliance, and the availability of any necessary upgrades.

Another source used to ascertain Y2K compliance of vendors' systems has been the Internet. One site maintained by a contractor of GSA provides information on the Y2K compliance of building systems. Contact information is provided indicating contact points should there be additional questions.

Business Contingency Plans

The BOP, due to its mission, has had formal emergency plans. These plans include steps to be taken should there be system failures. The remedial measures set forth within these plans do not necessarily address the handling of contingencies brought about by system failures due to non-Y2K compliance, but rather failure of systems without regard to the cause. These plans are being updated to specifically cite failures brought about solely due to Y2K non-compliance, but the corrective actions regarding operations contained in these plans should not change based on the fact responses are predicated on system failures without regard to cause.

These plans also provide contingencies for disruption of services provided by outside entities. One example would be the failure of the electrical distribution network of an electric utility. The BOP does not have the autonomy to necessarily correct Y2K non-compliance of outside entities, but is seeking to identify the likelihood of such disruptions occurring. Additionally, the existing plans account for disruptions to such outside systems.

Specific Findings

The various categories of systems had varying degrees of Y2K non-compliance. The information provided is based on the BOP's experience, and is not intended as necessarily reflecting what other organizations may find.

A high percentage of certain systems were found to be in need of upgrade to be Y2K compliant.

Personal computers used to run control software were often found to be in need of upgrade.

The BOP's computerized maintenance scheduling software was DOS based. This necessitated upgrade to a Y2K compliant, Windows based program.

Telephone Branch Exchanges (PBXs) were all in need of either upgrade or replacement.

Software and firmware upgrades were required for numerous energy management systems and HVAC controls.

There were certain categories of systems found that presented few, if any, problems.

Elevator controls were found to be Y2K compliant.

Package scanning machines were found to be Y2K compliant.

Only a small percentage of fire alarm systems were in need of upgrade, and these were limited to software upgrades.

Radio system infrastructure were found to be Y2K compliant, however, software upgrades for subscriber units (mobiles and portables) were required.

Closed circuit television (CCTV) systems were found to be Y2K compliant.

Perimeter detection systems were found to be Y2K compliant.

Future Activities

The BOP continues in its efforts to identify and correct systems that potentially may fail to operate in a satisfactory manner due to being Y2K non-compliant. The BOP has actively tried to provide links to resources related to Y2K through its own site on the Internet, and in conjunction with the Internet site maintained by the National Institute of Corrections. These on-going efforts are aimed at helping others through the sharing of information and resources.